

REMARKS

Claims 1-43 are pending in the application.

Title

The Examiner alleges that Applicants' title is too long.

The Applicants' title is changed herein to a title similar to that suggested by the Examiner. The Applicants respectfully request the objection to the title be withdrawn.

Claims 1-43 over Schneier

In the Office Action, claims 1-43 were rejected under 35 U.S.C. §102(b) as allegedly being anticipated by U.S. Patent No. 5,970,143 to Schneier ("Schneier"). The Applicants respectfully traverse the rejection.

Claims 1-27 recite a system and method comparing a nonce value of a received message with a largest nonce value yet seen.

The Office Action alleges that Schneier discloses comparing a nonce value of a received message with a largest nonce value yet seen at col. 16, lines 9-16. However, Schneier discloses at col. 16, lines 9-16 discloses a sequence number that is incremented every time an AOM message is generated. If the sequence numbers are received in order, i.e., if a sequence number is one greater than a stored sequence number, a current message is accepted (See Schneier, col. 16, lines 9-16). Thus, Schneier compares a nonce value with a previously received nonce value to determine if the nonce values are sequential. Schneier does **NOT NEED** to determine if a nonce value is a largest nonce value yet seen because the previous nonce value will **always** be the largest nonce value yet seen. Schneier fails to disclose comparing a nonce value of a received message with a largest nonce value yet seen, as recited by claims 1-27.

Moreover, Schneier's col. 16, lines 9-16 is an entire embodiment, **NOT** a step in a larger encryption scheme. Thus, Schneier fails to disclose or suggest combining steps disclosed in separate embodiments as the Office Action is relying on.

Claims 1-27 recite comparing the nonce value to an acceptance window in response to the nonce value not exceeding the largest nonce value yet seen.

As discussed above, Schneier fails to disclose a determination of a largest nonce value yet seen, as recited by claims 1-27.

The Office Action alleges Schneier discloses comparing the nonce value to an acceptance window in response to the nonce value not exceeding the largest nonce value yet seen at col. 16, lines 17-32. However, Schneier at col. 16, lines 17-32 discloses two separate embodiments. Schneier at col. 16, lines 17-32 discloses use of time windows, with an AOM message checked against a computer's time clock to determine if a message is fresh. Schneier at col. 16, lines 24-32 discloses use of random numbers that are associated with AOM messages that are checked against a database of random numbers previously received. Schneier at col. 16, lines 17-32 fails to even mention determination of a largest nonce value yet seen, much less comparing the nonce value to an acceptance window in response to the nonce value not exceeding the largest nonce value yet seen, as recited by claims 1-27.

Moreover, as discussed above, Schneier's col. 16, lines 17-23 and col. 16, lines 24-32 are separate embodiments, **NOT** steps in a larger encryption scheme. As discussed above, Schneier fails to disclose or suggest combining steps disclosed in separate embodiments as the Office Action is relying on.

Claims 28-43 recite a system and method of comparing a nonce value to a filter in response to a nonce value of a received packet not exceeding a largest nonce value yet seen.

The Office Action alleges that Schneier disclose at col. 16, lines 24-32 comparing a nonce value to a filter in response to a nonce value of a received packet not exceeding a largest nonce value yet seen. However as discussed above, Schneier fails to disclose a determination of a largest nonce value yet seen, much less a system and method of comparing a nonce value to a filter in response to a nonce value of a received packet not exceeding a largest nonce value yet seen, as recited by claims 28-43.

A benefit of a system and method comparing a nonce value of a received message and packet with a largest nonce value yet seen is, e.g., an ability to track replay attacks for out-of-order messages and packets. Schneier relies on a determination if messages have consecutive nonce values. However, consecutive nonce values are only applicable to messages that are received in-order. For out-of-order messages Schneier's method would be inadequate and result in a false determination of a replay attack. However, Applicants' claimed features account for out-of-order messages and packets for a determination of a replay attack. The cited prior art fails to disclose or suggest the claimed features having such benefits.

Accordingly, for at least all the above reasons, claims 1-43 are patentable over the prior art of record. It is therefore respectfully requested that the rejection be withdrawn.

Conclusion

All objections and rejections having been addressed, it is respectfully submitted that the subject application is in condition for allowance and a Notice to that effect is earnestly solicited.

Respectfully submitted,



William H. Bollman
Reg. No.: 36,457
Tel. (202) 261-1020
Fax. (202) 887-0336

MANELLI DENISON & SELTER PLLC

2000 M Street, NW 7TH Floor
Washington, DC 20036-3307
TEL. (202) 261-1020
FAX. (202) 887-0336

WHB/df